a certain person by including the public key of the person in question in the ticket, unsecure channels (such as email) can be used in distributing tickets. Even if someone else is able to copy the ticket, he cannot use it without knowing the secret key of the legitimate user.

Tickets are stored on key devices. The number of tickets a key device can store is limited by the amount of storage space (non-volatile memory) available.

Note that while creating keys requires access to the lock device, tickets can be created just by using a key device whose public key is stored in the lock device. It is even possible to create tickets that allow the creation of more tickets. The ticket holder simply creates a new ticket, signed with his own secret key, and appends the original ticket (a more detailed description is provided in the next section). This means that tickets are in fact equivalent to keys in terms of functionality - the only drawback is that more storage space is required in the key device.

Tickets can also contain additional information, i.e. information that is not related to the lock and key devices or access control. This additional information may contain user-related information such as e.g. user preferences.

Lock and key systems according to an embodiment of the invention can be used in addition to the traditional door opening applications, also in "virtual lock and key" systems wherein the "virtual lock" is a software module controlling access to digital resources such as e.g. to a computer and/or to a file therein or giving access to a database through a computer or another access device such as e.g. a PDA or a mobile phone. The access device and/or a data file and/or a database containing one or more data files can be 'locked' against unauthorized access and/or use. The idea is that the same key device that is used to access physical locks can also be used in connection

with access to virtual locks. Thus, the user uses his (physical) key device to open a virtual lock just as he would open a physical lock. The opening may happen automatically without user intervention, or user confirmation may be required, or the user may be required to additionally authenticate himself (to guard against stolen key devices) with a PIN, fingerprint, retinal scan or similar procedure.

A computer terminal and/or a device connected to it and/or a peripheral device can also be locked with a physical lock against unauthorized use or against unauthorized removal from their location or even against theft. Also opening of these locks is within the scope of the invention.

Brief Description of the Drawings

The present invention is more easily understood with reference to the drawings, in which:

Fig. 1 is an embodiment of the flowchart for opening a lock with a key, from the key device point of view.

Fig. 2 is an embodiment of the flowchart for opening a lock with a key, from the lock device point of view.

Fig. 3 is an embodiment of the flowchart for opening a lock with a ticket, from the key device point of view.

Fig. 4 is an embodiment of the flowchart for opening a lock with a ticket, from the lock device point of view.

Fig. 5 is an embodiment of the flowchart for verifying a ticket, from the lock device point of view.

Fig. 6 is an embodiment of the key for the different symbols in the flowcharts.

Detailed Description of the Preferred Embodiment

The basic environment of the embodiment of the present invention is to utilize an electronic key for wirelessly opening an electronic lock. The key is carried on a person either as part of his wireless telephone or as a separate unit which can be carried or worn on his person, such as in a belt buckle or in a piece of jewelry. When a person approaches the lock, his presence is sensed. Either the lock or the key may initiate the transaction. In a preferred embodiment the lock transmits a signal to see if a key is carried by the person. The lock sends a random data signal to the key. The key encrypts this data and sends it back to the lock. The lock decrypts the signal and, if it matches the original signal, opens the lock.

The encryption uses an encryption key pair system, with the public key being carried in the lock and the private key being carried in the key. This allows the user to use a single key for multiple locks. Thus, his public key may be stored in any number of locks, so that a single key is operational in all of them. Likewise, public keys of other people may also be stored in various locks, so that many people may be authorized to use the same lock.

In order to grant temporary access to a lock, a key may be given the authority to issue tickets to others which will also open the lock. These tickets may be used only a given number of times or may be used only at certain times of the day. Tickets can also be given the authority to grant additional tickets if desired. Tickets may have an expiration date if desired.

The embodiment of the present invention relies on the use of digital signatures to authenticate tickets. It further relies on chaining signatures in such a fashion that each signature authenticates the next one, to authenticate tickets created from other tickets